**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate and reliable, and is available in a timely manner.

1. Biometrics
   1. Describe biometric security.

Biometric security is the use of physical human characteristics, including fingerprints or facial features, or behavioural characteristics such as voice patterns or handwriting, to authenticate a user before granting them access to data.

* 1. Why does it appeal to security managers?

It appeals to security managers because it is nearly impossible to copy or steal a person’s biometric characteristics.

* 1. List the common biometric devices
* Voice recognition
* Fingerprint recognition
* Hand geometry
* Signature verification
* Facial recognition
* Iris recognition
  1. What are the concerns of biometric technology?

The main concern of users is the perceived intrusiveness of the technology.

1. Swipe cards
   1. Describe the nature of a swipe card.

Swipe cards are a common type of security device used by many people.

* 1. What is a limitation of the swipe card?

One limitation of a swipe card is that it can be easily damaged by magnetic fields.

1. Smart cards

Smart cards are very similar to the swipe cards, except that it has a microchip embedded in it to store and manipulate data.

1. Security tokens

Security tokens can constantly display the changing of authentication code. When the user wishes to access information, they need to enter their account name, their password and then the authentication code displayed on the security tokens.

1. Mobile phone secure code
   1. How does this level of authentication work?

Authentication occurs when a security code is sent to the account holder’s mobile phone to authenticate a transaction before it actually occurs.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

Surge protector can protects electrical equipment against overvoltage caused by a power surge.

1. Uninterruptible power supply, (UPS)

A UPS is a high-quality and battery built into the one device.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

Redundancy refers the protection of the system failures.

1. What is meant be a fault-tolerant server?
2. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

There are two main safeguards against system failures. One is using multiple hard drives or fault-tolerant equipment. One is through mirrored servers or machines.

* 1. What is meant by RAID technology

A RAID is normally used on a computer network. In a RAID-protected system, drive fails, the other can piece together the missing data and rebuild the disks has failed because the data is fixed rapidly.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

Mirrored servers are too expensive.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

Three categories of backup media: Magnetic media, optical drives, solid-state drives.

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

An affordable option is to back files in a second internal hard disk. This is useful if you have many files. It is best to have a removable or external hard drive, otherwise in the case of a disaster, such as a fire or flood, the backup drive may be destroyed along with the original.

1. Magnetic tapes

Magnetic tapes are a very popular form of media for backup files. They are relatively cheap, but very slow to save and restore files, as the tape must be read and accessed sequentially.

**Optical media**

1. Compact disc

Compact discs are removable storage media can hold up to 700MB of data and come either as CD-Read, which can only be used once to write data, or CD-RW which allows you to write data to the disc a number of times.

1. DVD

With a amount of data being stored within home and organisational computers growing rapidly, the popularity of the DVD as a backup medium has grown.

1. Blu-ray

Blu-ray is a new optical disc format with a capacity of 50GB designed to replace the DVD format.

**Solid-state drives**

1. USB storage devices

USB keys or storage devices are a popular way of backing of files. USB keys are small and often conveniently sold as a “key ring” that you can take anywhere.

**Online backups**

1. Why do organisations use this form of backup?

Larger organisation will often want to consolidate storage and backup systems to ensure that they work as efficiently and effectively as possible.

1. Describe an enterprise storage system.

An enterprise storage system typically involves the interconnection via a storage area network, RAID disks, CD/DVD-ROM servers, Internet backup and other networked storage devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

Packet sniffers are diagnostic tools that monitor the contents of packets of data being sent across networks.

1. Desktop monitoring programs

Desktop monitoring programs work by intercepting every single action performed on a computer. The monitoring program must be installed on the computer, but this can be done easily by an administrator either sitting at the programs to install this type of software.

1. Log files

Even without dedicated monitoring programs, computers already record most of what we do. Web servers record every URL accessed, who accessed it and how long they remained at that site.

1. Closed-circuit television, (CCTV)

CCTV consists of a series of video cameras linked to an internal TV system.

1. Telephones

Many spy films show secret agents listening in to or tapping telephone conversations. Employers will often do the same.

1. Audit trails

The combination of surveillance systems described above enable managers to trace transactions or any other form of activity in the system. This is called an audit trail. The audit trail would include log files of system logins, both successful and unsuccessful, as well as any files that were accessed, modifies or copied.

**Physical security devices:** List the options for physically securing your data